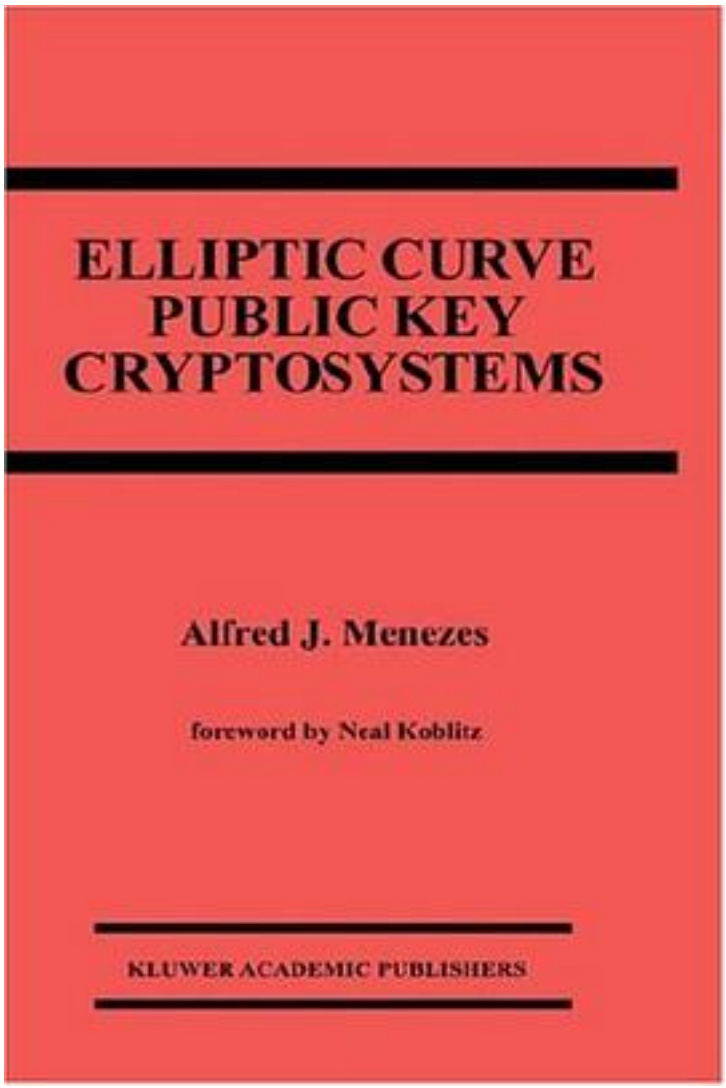
Elliptic Curve Public Key Cryptosystems (The Springer International Series in Engineering and Computer Science)



Elliptic Curve Public Key Cryptosystems (The Springer International Series in Engineering and Computer Science)_下载链接1_

著者:Alfred J. Menezes

出版者:Springer

出版时间:1993-07-31

装帧:Hardcover

isbn:9780792393689

Elliptic curves have been intensively studied in algebraic geometry and number theory. In recent years they have been used in devising efficient algorithms for factoring integers and primality proving, and in the construction of public key cryptosystems. Elliptic Curve Public Key Cryptosystems provides an up-to-date and self-contained treatment of elliptic curve-based public key cryptology. Elliptic curve cryptosystems potentially provide equivalent security to the existing public key schemes, but with shorter key lengths. Having short key lengths means smaller bandwidth and memory requirements and can be a crucial factor in some applications, for example the design of smart card systems. The book examines various issues which arise in the secure and efficient implementation of elliptic curve systems. Elliptic Curve Public Key Cryptosystems is a valuable reference resource for researchers in academia, government and industry who are concerned with issues of data security. Because of the comprehensive treatment, the book is also suitable for use as a text for advanced courses on the subject.

作者介绍:

目录:

Elliptic Curve Public Key Cryptosystems (The Springer International Series in Engineering and Computer Science)_下载链接1_

标签

评论

Elliptic Curve Public Key Cryptosystems (The Springer International Series in Engineering and Computer Science)_下载链接1_

书评

Elliptic Curve Public Key Cryptosystems (The Springer International Series in Engineering and Computer Science)_下载链接1_